

REMARKS

The present Amendment amends claim 8, leaves claim 9 unchanged and cancels claims 1-7 and 10-19. Therefore, the present application has pending claims 8 and 9.

Claims 1-7 and 11-19 stands provisionally rejected under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 20-35 of copending Application Serial No. 10/124,577. As indicated above, claims 1-7 and 11-19 were canceled. Therefore, this rejection is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

It should be noted that the cancellation of claims 1-7 and 11-19 was not intended nor should it be considered as an agreement on Applicants part that the features recited in claims 1-7 and 11-19 are taught or suggested by claims 20-35 of the copending application. The cancellation of claims 1-7 and 11-19 was simply intended to expedite prosecution of the present application.

Claims 1-19 stand rejected under 35 USC §101 as allegedly being directed to non-statutory subject matter. As indicated above, claims 1-7 and 10-19 were canceled. Therefore, this rejection with respect to claims 1-7 and 10-19 is rendered moot. This rejection with respect to the remaining claims 8 and 9 is traversed for the following reasons. Applicants submit that the features of the present invention as recited in claims 8 and 9 are clearly directed to an apparatus such as that illustrated, for example, in Fig. 2 of the present application. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In the Office Action the Examiner alleges that the claims are directed to functional descriptive material of a computer program. However, the Examiner is completely in error in this regard being that the specification clearly describes that the present invention can be implemented in hardware or software. The hardware implementation of the present invention is illustrated, for example, in Fig. 2. Therein, it is quite clear that the present invention provides specific well known elements which correspond to the elements recited in the claims. For example, the pseudorandom number generating apparatus corresponds to the pseudonumber generating apparatus 200, as illustrated in Fig. 1, which includes a state storage section 201, a buffer 202, a state transformation section 203 and a state storage control section and buffer control section 214. The specification clearly describes the buffer 202 as being a well known, real-world item which temporarily stores data. As understood by those of ordinary skill in the art a computer program cannot in of itself perform any buffering type functions or storage since it merely corresponds to lines of codes or instructions.

Further, it is well known by those of ordinarily skill in the art that signal processing type inventions can be, and often times are, implemented by hardware only even though a software implementation is possible. The specification clearly describes that the inventors contemplated both the hardware and software implementations of their invention at the time the invention was made. Claims 8 and 9 are simply directed to hardware implementation of their invention as illustrated in Figs. 2-6 and discussed in the corresponding portions of the specification.

Thus, the claims are directed to a machine which is one of the statutorily defined classes of patentable subject matter and as such are not prohibited by 35 USC §101. Therefore, reconsideration and withdrawal of the 35 USC §101 rejection of claims 8 and 9 is respectfully requested.

Claims 1, 7-10, 14 and 19 stand rejected under 35 USC §102(b) as being anticipated by Daemen (article entitled "Fast Hashing and Stream Encryption with PANAMA"). As indicated above, claims 1, 7, 10, 14 and 19 were canceled. Therefore, this rejection with respect to claims 1, 7, 10, 14 and 19 is rendered moot.

This rejection with respect to claims 8 and 9 is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 8 and 9 are not taught or suggested by Daemen whether taken individually or in combination with any of the other references of record. Therefore, reconsideration and withdrawal of this rejection with respect to claims 8 and 9 is respectfully requested.

The present invention is directed to an encryption and decryption apparatuses as recited in claims 8 and 9.

The encryption apparatus includes a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of plaintext data to be encrypted and an operation section for conducting an exclusive OR-ing operation on the generated pseudorandom number sequence and the plaintext data, thereby calculating ciphertext data and outputting the ciphertext data.

The pseudorandom number generating apparatus includes a state storage section, a buffer, a state transformation section for conducting

transformation using a storage content of the buffer and a storage content of the state storage section and outputting a result of the transformation, a state storage control section for updating an internal state of the state storage section by using the output of the state transformation section according to a clock and a buffer control section for updating an internal state of the buffer by using the output of the buffer transformation section.

According to the present invention the state storage section has a capacity of three blocks (where one block has n bits), and the buffer has a capacity of a plurality of blocks, and wherein the state transformation section includes a nonlinear transformation section that uses the storage content of the buffer and the storage content of the state storage section as inputs and an output section for outputting one block data included in the result of the transformation as a partial random number sequence.

The decryption apparatus as recited in claim 9 recites features similar to those of the encryption apparatus recited in claim 8.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly, the above described features of the present invention as now more clearly recited in claims are not taught or suggested by Daemen whether taken individually or in combination with any of the other references of record.

Daemen, teaches a cryptographic module that can be used both as a cryptographic hash function and as a stream cipher. As taught by Daemen high performance is achieved through a combination of low work-factor and a

high degree of parallelism. Throughputs of 5.1 bits/cycle for the hashing mode and 4.7 bits/cycle for the stream cipher mode are demonstrated on a commercially available VLIW micro-processor. In Daemen the PANAMA structure has a finite state machine with a 544-bit state and a 8192-bit buffer with 32 stages each consisting of 8 words (see page 61). However, Daemen fails to teach or suggest numerous features of the present invention as recited in claims 8 and 9.

Particularly, Daemen fails to teach the features of the present invention as recited in claim 8 that the state storage section has a capacity of 3 blocks (where one block has n bits), and the buffer has a capacity of a plurality of blocks. These features, among other features, of the present invention provides a benefit not possible in Daemen. Attention is directed to the description of the present invention as set forth on page 12, lines 15-25 (also refer to the Abstract) of the present application, wherein the passage states:

"From the viewpoint of the digital circuit or program structure, it is desirable to use a multiple of 32 as the unit of processing. From the viewpoint of cryptographic security, it is desired that the number of internal states of the state and the buffer is large. In the present preferred embodiment, one block serving as the unit of processing is set equal to 64 bits. The size of the state is set equal to 3 blocks, and the size of the buffer is set equal to 32 blocks. As a result, it becomes possible to parallelize the processing and make the circuit scale small." (emphases added)

In addition, the present invention could provide the higher security in the high-speed pseudorandom number generator as discussed, for example, at page 6, line 2 through page 7, line 9, wherein the passage states:

"In the above-described configuration, parallel processing is made possible by setting the size of the state equal to at least 3 blocks by n bits. In addition, by setting the size of the state equal to 3 blocks by n bits, it becomes possible to make the circuit scale small at the time of hardware implementation. In other words, the above-described configuration makes it possible to implement a pseudorandom number generating apparatus having the following advantages:

(a) higher security can be ensured though security evaluation is simple;

(b) the speed in software implementation and hardware implementation is high; and

(c) the required memory region and the number of gates in hardware implementation are small, and the implementation cost is low." (emphasis added)

Based on the above it is clear that even if a skilled artisan attempted to apply the three(3) word scheme in equation (4) in page 62 of the present application to the teachings in Daemen, it will not be possible to hold surjection or injection (one-to one mapping), thereby causing a loss of security in the system.

Thus, Daemen fails to teach or suggest that the state storage section has a capacity of three blocks, wherein one block has n bits, and the buffer has a capacity of a plurality of blocks and that the state transformation section includes a nonlinear transformation section that uses the storage content of the buffer and the storage content of the state storage section as inputs and an output section for outputting one block data included in the result of the transformation as a partial number sequence as recited in the claims.

Therefore, Daemen fails to teach or suggest the features of the present invention as now more clearly recited in claims 8 and 9. Accordingly,

reconsideration and withdrawal of the 35 USC §102(b) rejection of claims 8 and 9 as being anticipated by Daemen is respectfully requested.

Applicants acknowledge the Examiner's indication in paragraph 11 of the Office Action that claims 2-6, 11-13 and 16-18 would be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims and further rewritten to overcome the 35 USC §101 and double patent rejection. However, as indicated above, claims 2-6, 11-13 and 16-18 were canceled and were added to the copending application Serial No. 10/124,577 as new claims 36-51. Therefore, the Examiner's indication that these claims would be allowable still applies to said claims, but should be reconfirmed by the Examiner in the copending application.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the reference utilized in the rejection of claims 1, 7-10, 14 and 19.

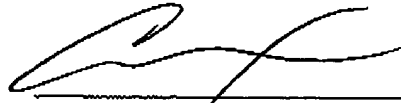
In view of the foregoing amendments and remarks, applicants submit that claims 8 and 9 are in condition for allowance. Accordingly, early allowance of claims 8 and 9 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any

overpayment of fees, to the deposit account of MATTINGLY, STANGER,
MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (500.41083X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120